LISTING OF CLAIMS

Claims 1-53 are presented for examination. No claims have been amended, canceled, or added. This listing is of the claims as currently pending.

1. (Previously Presented) A device for connection to a data processing apparatus, the device including

authentication storage means operatively coupled thereto for storing predetermined authentication information respective to a user,

the authentication storage means being registered with a telecommunications system which includes authenticating means and for which the user has a telecommunications terminal,

the device, when operatively coupled to the authentication storage means, being responsive to an input message for deriving a response dependent on the input message and on the authentication information for enabling the authenticating means to carry out an authentication process via a communication link with the authenticating means in the telecommunications system whereby to authenticate a subsequent transaction by the user with the data processing apparatus and which involves use of the data carried by the authentication storage means,

the predetermined authentication information stored by the authentication storage means corresponding to information which is used to authenticate the user registered with the telecommunications system in relation to use of that user's telecommunications terminal in the telecommunications system,

but the authentication process for authenticating the transaction by that user with the data processing apparatus not requiring use of the user's telecommunications terminal nor requiring the telecommunications terminal to be actually authenticated by that information in relation to

the telecommunications system, and wherein the device controls access to the authentication information.

2. (Previously Presented) The device of claim 1, comprising security data entry means for obtaining security data independently of the data processing apparatus, and means for analyzing the entered security data for determining whether to allow access to the predetermined information.

3. (Previously Presented) The device of claim 2, wherein the security data entry means comprises alphanumeric data entry means.

4. (Previously Presented) The device of claim 2, wherein the security data entry means comprises a keypad.

5. (Previously Presented) The device of claim 2, wherein the security data comprises a Personal Identification Number (PIN) and the analyzing means compares the PIN obtained by the security data entry means with a PIN stored on the authentication storage means and only allows access to the predetermined information when the respective PINs match.

6. (Previously Presented) The device of claim 1, comprising a display for displaying security information.

7. (Previously Presented) The device of claim 1, comprising a data processing module for controlling the communication with the data processing apparatus.

8. (Previously Presented) The device of claim 7, wherein the data processing module of the device is configured for communicating with a corresponding data processing module of the data processing apparatus.

9. (Previously Presented) The device of claim 8, wherein communication between the authentication storage means and the data processing apparatus is performed via the respective data processing modules.

10. (Previously Presented) The device of claim 7, wherein the data processing module of the device includes means for decrypting encrypted data received from the data processing module of the data processing apparatus.

11. (Previously Presented) The device of claim 7, wherein the data processing module of the device includes means for encrypting data transmitted to the data processing module of the data processing apparatus.

12. (Previously Presented) The device of claims 10, wherein the respective data processing modules comprise a key for allowing encryption and/or decryption of data.

13. (Previously Presented) The device of claim 12, wherein the key comprises a shared secret key for each of the respective data processing modules.

14. (Previously Presented) The device of claim 1, in which each user is authenticated in the telecommunications system by use of a subscriber identity module, and in which the authentication storage means respective to that user corresponds to or simulates the subscriber identity module for that user.

15. (Previously Presented) The device of claim 1, in which the transaction is a transaction involving use of data processing functions of the data processing apparatus.

16. (Previously Presented) The device of claim 1, in which the authentication storage means is specific to that device.

17. (Previously Presented) The device of claim 1, in which the authentication process involves the sending of a message and the generation of a response dependent on the message and the predetermined information.

18. (Previously Presented) The device of claim 14, wherein the telecommunications system includes means for levying a charge for the transaction when authorised.

19. (Previously Presented) The device of claim 1 in combination with the data processing apparatus .

20. (Previously Presented) The device of claim 1 in combination with the telecommunications system.

21. (Previously Presented) A method for authenticating a transaction with a data processing apparatus in which the data processing apparatus has operatively associated with it a security device which in turn has operatively associated with it authentication storage means for storing predetermined authentication information respective to a user,

the authentication storage means being registered with a telecommunications system which includes authenticating means and for which the user has a telecommunications terminal,

the device, when operatively coupled to the authentication storage means, being responsive to an input message for deriving a response dependent on the input message and on the authentication information for enabling the authenticating means to carry out an authentication process via a communication link with the authenticating means in the telecommunications system whereby to authenticate a subsequent transaction by the user with the data processing apparatus and which involves use of the data carried by the authentication storage means,

the predetermined authentication information stored by the authentication storage means corresponding to information which is used to authenticate the user registered with the

telecommunications system in relation to use of that user's telecommunications terminal in the telecommunications system,

the predetermined authentication information being obtained from the authentication storage means via the security device which controls access to the predetermined authentication information,

but the authentication process for authenticating the transaction by that user with the data processing apparatus not requiring use of the user's telecommunications terminal nor requiring the telecommunications terminal to be actually authenticated by that information in relation to the telecommunications system, and wherein the device controls access to the authentication information.

22. (Previously Presented) The method of claim 21, comprising obtaining security data independently of the data processing apparatus, and analyzing the security data for determining whether to allow access to the predetermined information.

23. (Previously Presented) The method of claim 22, wherein the security data is obtained by alphanumeric data entry means.

24. (Previously Presented) The method of claim 23, wherein the alphanumeric data entry means (46) comprises a keypad.

25. (Previously Presented) The method of claim 22, wherein the security data comprises a Personal Identification Number (PIN) and the analyzing step compares the PIN obtained by the security data entry means with a PIN stored on the authentication storage means (12) and only allows access to the predetermined information when the respective PINs match.

26. (Previously Presented) The method of claim 21, comprising displaying security information.

27. (Previously Presented) The method of claim 21, wherein communication with the data processing apparatus is controlled by a data processing module.

28. (Previously Presented) The method of claim 27, wherein the data processing module of the device is configured for communicating with a corresponding data processing module of the data processing apparatus.

29. (Previously Presented) The method of claim 28, wherein communication between the authentication storage means and the data processing apparatus is performed via the respective data processing modules.

30. (Previously Presented) The method of claim 27, wherein the data processing module of the device decrypts encrypted data received from the data processing module of the data processing apparatus.

31. (Previously Presented) The method of claim 27, wherein the data processing module of the device encrypts data transmitted to the data processing module of the data processing apparatus.

32. (Previously Presented) The method of claim 30, wherein the respective data processing modules comprise a key for allowing encryption and/or decryption of data.

33. (Previously Presented) The method of claim 32, wherein the key comprises a shared secret key for each of the respective data processing modules.

34. (Previously Presented) A method according to claim 21, in which each user is authenticated in the telecommunications system by means of use of a subscriber identity module, and in which the authentication storage means respective to that user corresponds to or simulates the subscriber identity module for that user.

35. (Previously Presented) A method according to claim 21, in which the transaction is a transaction involving use of the data processing functions of the data processing apparatus.

36. (Previously Presented) A method according to claim 21, in which each authentication storage means is associated with a specific security device.

37. (Previously Presented) A method according to claim 21, in which the authentication storage means is associated with the data processing apparatus by being associated with data or software for use by that data processing apparatus.

38. (Previously Presented) A method according to claim 21, in which the authentication process involves the sending of a message and the generation of a response dependent on the message and the predetermined information.

39. (Previously Presented) A method according to claims 21, including the step of levying a charge for the transaction when authenticated.

40. (Previously Presented) A method according to claim 39, in which the step of levying the charge is carried out by the said telecommunication system.

41. (Previously Presented) A method according to claim 21, in which the data processing apparatus is a personal computer.

42. (Previously Presented) A device including authentication storage means for controlling access to predetermined authentication information stored on the authentication storage means,

the device including means for coupling the device to a data processing apparatus to allow the authentication information to be used to authenticate a transaction performed by the data processing apparatus,

the predetermined authentication information stored on the authentication storage means being respective to a user, the authentication storage means being registered with a telecommunications system which includes authenticating means and for which the user has a telecommunications terminal,

the device, when operatively coupled to the authentication storage means, being responsive to an input message for deriving a response dependent on the input message and on the authentication information for enabling the authenticating means to carry out an authentication process via a communication link with the authenticating means in the telecommunications system whereby to authenticate the transaction by the user with the data processing apparatus, and

wherein security means is provided for controlling access to the authentication information via the data processing apparatus,

but the authentication process for authenticating the transaction by that user with the data processing apparatus not requiring use of the user's telecommunications terminal nor requiring the telecommunications terminal to be actually authenticated by that information in relation to the telecommunications system, and wherein the device controls access to the authentication information.

43. (Previously Presented) The device of claim 42, wherein the security means comprises means for obtaining security data from a user and means for checking the validity of the security data and only allowing access to the authentication data if the security data is valid.

44. (Previously Presented) The device of claim 42, wherein the security means comprises data processing means for receiving an encrypted authentication request, encrypted using a predetermined key, from the data processing apparatus and for decrypting the request.

45. (Previously Presented) The device of claim 44 in combination with the data processing apparatus, wherein the data processing apparatus comprises means for encrypting the authentication request using said key.

46. (Previously Presented) A device according to claim 1, wherein the device communicates wirelessly to authenticate the transaction.

47. (Previously Presented) A device according to claim 14, wherein the subscriber identity module authenticates the transaction when the subscriber identity module is operable in a mobile terminal.

48. (Previously Presented) A device according to claim 14, wherein the subscriber identity module is further operable to authenticate a mobile terminal for use in the system.

49. (Previously Presented) A method according to claim 21, wherein the security device communicates wirelessly to authenticate the transaction.

50. (Previously Presented) A method according to claim 34, wherein the subscriber identity module authenticates the transaction when the subscriber identity module is operable in a mobile terminal.

51. (Previously Presented) A method according to claim 34, wherein the subscriber identity module is further operable to authenticate a mobile terminal for use in the system.

52. (Previously Presented) The method of claims 31, wherein the respective data processing modules comprise a key for allowing encryption and/or decryption of data.

53. (Previously Presented) A device according to claim 42, wherein the device communicates wirelessly to authenticate the transaction.